JIANGSU UNIVERSITY, SCHOOL OF COMPUTER SCIENCE AND COMMUNICATION ENGINEERING

Cryptography_exercise

Students

November 6, 2016

1. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p , substitute the ciphertext letter C:

$$C = E([a, b], p) = (ap + b) \bmod 26$$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$,then $E(k,p) \neq E(k,q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a=2 and b=3,then E([a,b],0)=E([a,b],13)=3.
a. Are there any limitations on the value of b Explain why or why not.
b. Determine which values of are not allowed.
c. Provide a general statement of which values of a are and are not allowed. Justify your statement.

ANSWER:
a. No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.
b. 2,4,6,8,10,12,13,14,16,18,20,22,24. Any value of a larger than 25 is equivalent to a mod 26.
c. The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that E(a,p) = E(a,q) ($0 \leq p \leq q < 26$) if and only if a(p-q) is divisible by 26.
(1). Suppose that a and 26 are relatively prime. Then, a(p-q) is not divisible by 26, because there is no way to reduce the fraction a/26 and (p-q) is less than 26.
(2). Suppose that a and 26 have a common factor k>1. Then E(a,p)=E(a,q), if $q = p + m/k \neq p$.

2. A ciphertext has been generated with an affine cipher.The most frequent letter of the ciphertext is B, and the second most frequent letter of the ciphertext is U. Break this code.
ANSWER:Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t = 19; U = 20. Then we have the following equations:

$$1 = (4a + b) \bmod 26$$
$$20 = (19a + b) \bmod 26$$

Thus, 19 = 15a mod 26. By trial and error, we solve: a = 3. Then 1 = (12 + b) mod 26. By observation, b = 15.
3. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. The particular scheme discussed in this problem is from one of the best suspense novels involving secret codes, Talking to Strange Men, by Ruth Rendell. Work this problem without consulting that book!Consider the following message:

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

This ciphertext was produced using the first sentence of The Other Side of Silence(a book about the spy Kim Philby):The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.
A simple substitution cipher was used.
a. What is the encryption algorithm?
b. How secure is it?
c. To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?

ANSWER:a.The first letter t corresponds to A, the second letter h corresponds to B, e is C, s is D, and so on. Second and subsequent occurrences of a letter in the key sentence are ignored. The result:
ciphertext: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
plaintext: basilisk to leviathan blake is contact
b. It is a monalphabetic cipher and so easily breakable.
c. The last sentence may not contain all the letters of the alphabet. If the first sentence is used, the second and subsequent sentences may also be used until all 26 letters are encountered.

4. Using the VigenÍÍre cipher, encrypt the word ąřexplanationąś using the key leg.

ANSWER:key: legleglegle
plaintext: explanation
ciphertext: PBVWETLXOZR

5. It can be shown that the Hill cipher with the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{0.1}$$

requires that is relatively prime to 26; that is, the only common positive integer factor of and 26 is 1. Thus, if or is even, the matrix is not allowed. Determine the number of different (good) keys there are for a 2 ąÁ 2 Hill cipher without counting them one by one, using the following steps:
a. Find the number of matrices whose determinant is even because one or both rows are even. (A row is ąřevenąś if both entries in the row are even.)
b. Find the number of matrices whose determinant is even because one or both columns are even. (A column is ąřevenąś if both entries in the column are even.)
c. Find the number of matrices whose determinant is even because all of the entries are odd.
d. Taking into account overlaps, find the total number of matrices whose determinant is even.
e. Find the number of matrices whose determinant is a multiple of 13 because the first column is a multiple of 13.
f. Find the number of matrices whose determinant is a multiple of 13 where the first column is not a multiple of 13 but the second column is a multiple of the first modulo 13.
g. Find the total number of matrices whose determinant is a multiple of 13.
h. Find the number of matrices whose determinant is a multiple of 26 because they fit cases parts (a) and (e), (b) and (e), (c) and (e), (a) and (f), and so on.
i. Find the total number of matrices whose determinant is neither a multiple of 2 nor a multiple of 13.

ANSWER:
a.7×13^4
b.7×13^4
c.13^4
d.10×13^4
e.24×13^2
f.$24\times (13^2\text{-}1)$
g.37648
h.23530
i.157248

6. Consider a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given k,the key scheduling algorithm determines values for the first eight round keys,k1,k2 and then sets:

k9=k8,k10=k7,k11=k6.....k16=k1

Suppose you have a ciphertext c. Explain how, with access to an encryption oracle,you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the

device are not known to you and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)

ANSWER:Because of the key schedule, the round functions used in rounds 9 through 16 are mirror images of the round functions used in rounds 1 through 8. From this fact we see that encryption and decryption are identical. We are given a ciphertext c. Let m' = c. Ask the encryption oracle to encrypt m'. The ciphertext returned by the oracle will be the decryption of c.

7. Question:Briefly describe AddRoundKey .

Answer:
Key expansion:
W0 = 1010 0111 W1 = 0011 1011 W2 = 0001 1100 W3 = 0010 0111
W4 = 0111 0110 W5 = 0101 0001
Round 0:
After Add round key: 1100 1000 0101 0000
Round 1:
After Substitute nibbles: 1100 0110 0001 1001
After Shift rows: 1100 1001 0001 0110
After Mix columns: 1110 1100 1010 0010
After Add round key: 1110 1100 1010 0010
Round 2:
After Substitute nibbles: 1111 0000 1000 0101
After Shift rows: 0111 0001 0110 1001
After Add round key: 0000 0111 0011 1000

8. Question:For the ECB, CBC, and CFB modes, the plaintext must be a sequence of one or more complete data blocks (or, for CFB mode, data segments). In other words, for these three modes, the total number of bits in the plaintext must be a positive multiple of the block (or segment) size. One common method of padding, if needed, consists of a 1 bit followed by as few zero bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?

Answer:After decryption, the last byte of the last block is used to determine the amount of padding that must be stripped off. Therefore there must be at least one byte of padding.

9. Question:In the subsection on implementation aspects, it is mentioned that the use of tables helps thwart timing attacks. Suggest an alternative technique.

Answer:The primary issue is to assure that multiplications take a constant amount of time, independent of the value of the argument. This can be done by adding no-operation cycles

as needed to make the times uniform.

10. An early proposal for a digital signature scheme using symmetric encryption is based on the following. To sign an n-bit message, the sender randomly generates in advance 2n56-bit cryptographic keys :

$$k1\ ,\ K1\ ,\ k2\ ,\ K2\ ,\ \ldots\ ,\ kn\ ,\ Kn$$

which are kept private. The sender prepares in advance two sets of corresponding non-secret 64-bit validation parameters, which are made public :

$$u1,\ U1\ ,\ u2\ ,\ U2\ ,\ \ldots\ ,\ un\ ,\ Un \text{ and } v1\ ,\ V1\ ,\ v2\ ,\ V2\ ,\ \ldots\ ,\ vn\ ,\ Vn$$

where čž

$$vi = E\ (\ ki\ ,\ ui\ )\ ,\ Vi = E\ (\ ki\ ,\ Ui\ )$$

The message M is signed as follows. For the ith bit of the message, either ki or Ki is attached to the message, depending on whether the message bit is 0 or 1. For example, if the first three bits of the message are 011, then the first three keys of the signature are $k1$, $K2$, $K3$.

a. How does the receiver validate the message?
b. Is the technique secure?
c. How many times can the same set of secret keys be safely used for different messages?
d. What,if any,practical problems does this scheme present?

ANSWER:
a. The receiver validates the digital signature by ensuring that the first 56-bit key in the signature will encipher validation parameter $u1$ into E($k1$, $u1$) if the first bit of M is 0, or that it will encipher $U1$ into E($K1$, $U1$) if the first bit of M is 1; the second 56-bit key in the signature will encipher validation parameter $u2$ into E($k2$, $u2$) if the second bit of M is 0, or it will encipher $U2$ into E($K2$, $U2$) if the second bit of M is 1,; and so on.
b. Only the sender, who knows the private values of ki and Ki and who originally creates vi and Vi from ui and Ui can disclose a key to the receiver. An opponent would have to discover the value of the secret keys from the plaintext-ciphertext pairs of the public key, which was computationally infeasible at the time that 56-bit keys were considered secure.
c. This is a one-time system, because half of the keys are revealed the first time.
d. A separate key must be included in the signature for each bit of the message resulting in a huge digital signature.

11. The **DSS** document includes a recommended algorithm for testing a number for primality. (1). **[Choose w]** Let w be a random odd integer. Then (w - 1) is even and can be expressed in the form $2^a m$ with odd. That is, 2^a is the largest power of 2 that divides (w - 1).
(2). **[Generate b]** Let b be a random integer in the range $1 < b < w$.
(3). **[Exponentiate]** Set j = 0 and z =b^m mod w.
(4). **[Done ?]** If $j = 0$ and $z = 1$, or if $z = (w - 1)$, then w passes the test and may be prime;go to step8.
(5). **[Terminate ?]** If $j > 0$ and $z = 1$, then w is not prime; terminate algorithm for this w.
(6). **[Increase j]** Set $j = j + 1$. If $j < a$,set $z = z^2$ mod w and go to step4.

(7). **[Terminate]** w is not prime;terminate algorithm for this w.
(8). **[Test again ?]** If enough random values of b have been tested, then accept w as prime and terminate algorithm; otherwise,go to step 2.

a. Explain how the algorithm works.
b. Show that it is equivalent to the Miller-Rabin test description.

ANSWER:
a. Note that at the start of step 4.The idea underlying this algorithm is that if $(b^m mod w) \neq 1$ and $w = 1 + 2^a m$ is prime, the sequence of values:

$$b^m \bmod w,\ b^{2m} \bmod w,\ b^{4m} \bmod w, \ldots$$

will end with 1, and the value just preceding the first appearance of 1 will be w - 1. Why? Because, if w is prime, then if we have $z^2 \bmod w = 1$, then we have $z^2 \equiv 1 \bmod w$. And if that is true, then $z = ((w - 1)$ or $z = (w + 1)$. We cannot have $z = (w + 1)$, because on the preceding step, z was calculated mod w, so we must have $z = (w - 1)$. On the other hand, if we reach a point where $z = 1$, and z was not equal to $(w - 1)$ on the preceding step, then we know that w is not prime.
b. This algorithm is a simplified version of the Miller-Rabin algorithm. In both cases, a test variable is repeatedly squared and computed modulo the possible prime, and the possible fails if a value of 1 is encountered.

12. It is tempting to try to develop a variation on Diffie-Hellman that could be used as a digital signature. Here is one that is simpler than DSA and that does not require a secret random number in addition to the private key.
Public elements: q prime number , α $\alpha < q$ and α is a primitive root of q
Private key: X $X < q$
Public key: $Y = \alpha^X \bmod q$
To sign a message M, compute h = h(M), which is the hash code of the message.We require that $gcd(h, q-1) = 1$.If not,append the hash to the message and calculate a new hash. Continue this process until a hash code is produced that is relatively prime to $(q - 1)$.Then calculate Z to satisfy $Z \times h \equiv X(mod q - 1)$.The signature of the message is α^Z. To verify the signature, a user verifies that $y = (\alpha^Z)^h = \alpha^X \bmod q$.

a. Show that this scheme works.That is, show that the verification process produces an equality if the signature is valid.
b. Show that the scheme is unacceptable by describing a simple technique for forging a userąs signature on an arbitrary message.

ANSWER:
a. To verify the signature, the user verifies that $(g^Z)^h = g^X mod p$.
b. To forge the signature of a message, I find its hash h. Then I calculate Υ to satisfy $\Upsilon h =$ 1 mod (p-1). Now $g^{\Upsilon h} = g$, so $g^{X\Upsilon h} = g^X mod p$. Hence $(h, g^{X\Upsilon})$ is a valid signature and the opponent can calculate $g^{X\Upsilon}$ as $(g^X)^\Upsilon$.

13. Suppose that, in PCBC mode, blocks C_i and C_{i+1} are interchanged during transmission. Show that this affects only the decrypted blocks P_i and P_{i+1} but not subsequent blocks.

ANSWER:
Let us consider the case of the interchange of C1 and C2. The argument will be the same for any other adjacent pair of ciphertext blocks. First, if C1 and C2 arrive in the proper order: $P_1 = E[K, C_1] \bigoplus IV$
$P_2 = E[K, C_2] \bigoplus C_1 \bigoplus P_1 = E[K, C_2] \bigoplus C_1 \bigoplus E[K, C_1] \bigoplus IV$
$P_3 = E[K, C_3] \bigoplus C_2 \bigoplus P_2 = E[K, C_3] \bigoplus C_2 \bigoplus E[K, C_2] \bigoplus C_1 \bigoplus E[K, C_1] \bigoplus IV$
Now suppose that C_1 and C_2 arrive in the reverse order. Let us refer to the decrypted blocks as Q_i. $Q_1 = E[K, C_2] \bigoplus IV$
$Q_2 = E[K, C_1] \bigoplus C_2 \bigoplus Q1 = E[K, C_1] \bigoplus C_2 \bigoplus E[K, C_2] \bigoplus IV$
$Q_3 = E[K, C_3] \bigoplus C_1 \bigoplus Q2 = E[K, C_3] \bigoplus C_1 \bigoplus E[K, C_1] \bigoplus C_2 \bigoplus E[K, C_2] \bigoplus IV$
The result is that Q_1 ąŮ P_1; Q_2 ąŮ P_2; but $Q_3 = P_3$. Subsequent blocks are clearly unaffected.

14. What are three threats associated with user authentication over a network or Internet?

ANSWER:
(1). A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
(2). A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
(3). A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

15. The 1988 version of X.509 lists properties that RSA keys must satisfy to be secure given current knowledge about the difficulty of factoring large numbers.The discussion concludes with a constraint on the public exponent and the modulus :
It must be ensured that $e > log_2(n)$to prevent attack by taking the eth root mod n to disclose the plaintext. Although the constraint is correct,the reason given for requiring it is incorrect.What is wrong with the reason given and what is the correct reason?

ANSWER:
Taking the eth root mod n of a ciphertext block will always reveal the plaintext, no matter what the values of e and n are. In general this is a very difficult problem, and indeed is the reason why RSA is secure. The point is that, if e is too small, then taking the normal integer eth root will be the same as taking the eth root mod n, and taking integer eth roots is relatively easy.

16. compute $3^{19935} \bmod 77$

$n = 11 * 7$
$\varphi(n) = 10 * 6 = 60$
$a^{\varphi(n)} = 1 \bmod n$
$3^{19935} \bmod 77 = 3^{332*60+15} \bmod 77 = 1 * 3^{15} \bmod 77 = 34$

17. Let the two communication sides use the RSA encryption system, the receiver's public key is (5,35), the received cipher text is 10, seeking the clear text.

$e = 5, n = 35, c = 10$
$\varphi(n) = \varphi(35) = \varphi(5)\varphi(7) = 4 * 6 = 24$
$d = e^{-1} \bmod \varphi(n) = 5^{-1} \bmod 24 = 5$
$m = c^d \bmod n = 10^5 \bmod 35 = 5$

18. Determine gcd(24140, 16762).

$gcd(24140, 16762) = gcd(16762, 7378)$
$= gcd(7378, 2006) = gcd(2006, 1360)$
$= gcd(1360, 646) = gcd(646, 68)$
$= gcd(68, 34) = gcd(34, 0)$
$= 34$